METHOD AND APPARATUS FOR PERFORMING MODULAR DIVISION USING COUNTERS

ABSTRACT

One embodiment of the present invention provides a system that performs modular division. This system contains a number of registers, including: a register A that is initialized with a value X; a register U that is initialized with a value Y; a register B that is initialized with a value M; and a register V that is initialized with a value 0. The system also includes a counter CA that indicates an upper bound for the most-significant non-zero bit of register A. It also includes a counter CB that indicates an upper bound for the most-significant non-zero bit of register B. The system additionally includes a temporary register H, and a temporary register L. An updating mechanism is configured to iteratively reduce the contents of registers A and B to a value of one by applying a plurality of operations to registers A, B, U and V. During operation, this updating mechanism temporarily stores $A + B$ in the temporary register H, and temporarily stores $U + V$ in the temporary register L. Moreover, the updating mechanism is configured to use counters CA and CB to estimate the relative magnitudes of the values stored in registers A and B instead of performing an expensive comparison operation between register A and register B.